

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-238306

(43)Date of publication of application : 31.08.1999

(51)Int.Cl. 611B 20/10
611B 19/04
// 611B 7/00

(21)Application number : 10-038840

(71)Applicant : FUJITSU LTD

(22)Date of filing : 20.02.1998

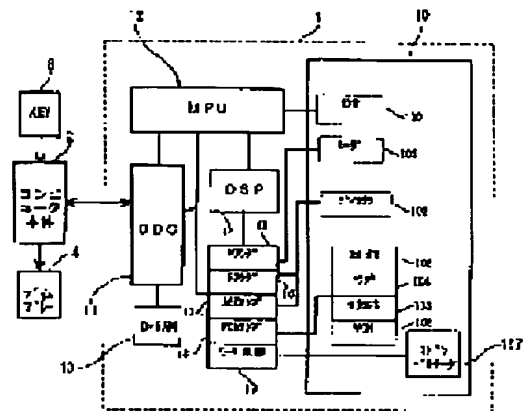
(72)Inventor : IMAMURA KIYOMI
YAMAKAWA TERUJI

(54) INFORMATION STORAGE DEVICE AND CONTROL METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To secure the secrecy of recorded data of a storage medium by making an information storage device impossible to get access to data of an inserted storage medium when the intrinsic identification sign of the information storage device which is previously recorded in the prescribed area of the storage medium and the identification sign of the storage device into which the storage medium is inserted do not coincide.

SOLUTION: Relating to a data storage device 1, an MPU 12 controls the whole of the device and a magneto-optical disk control part (ODC) 11 reads out the identification sign of the medium management information of an inserted magneto-optical disk to perform a security processing. When the identification signal is in an initial state, the ODC 11 permits the reading/writing of data and when data are written on the disk, the ODC 11 judges whether the sign of the disk coincides with that of the data storage device 1 or not. As a result, when they coincide, the ODC 11 permits the reading/writing of data, however, when they do not coincide, it inhibits the reading/writing of data. Thus, even when the inserted magneto-optical disk is plagiarized, the secrecy of the data is secured.



LEGAL STATUS

[Date of request for examination] 28.03.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-238306

(43) 公開日 平成11年(1999) 8月31日

(51) Int.Cl.⁹
G 1 1 B 20/10
19/04
// G 1 1 B 7/00

識別記号
5 0 1

F I
G 1 1 B 20/10
19/04
7/00
H
5 0 1 H
Q

審査請求 未請求 請求項の数36 O L (全 22 頁)

(21) 出願番号 特願平10-38840
(22) 出願日 平成10年(1998) 2月20日

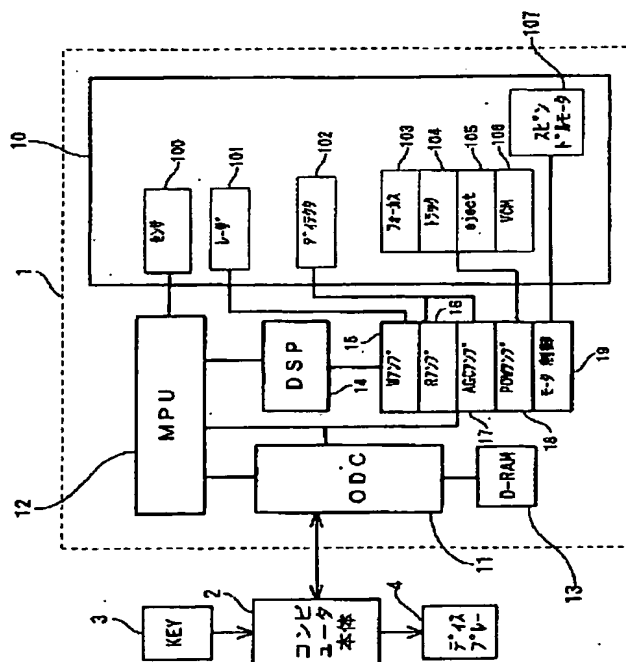
(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番
1号
(72) 発明者 今村 紀代美
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(72) 発明者 山川 輝二
神奈川県横浜市港北区新横浜2丁目4番19
号 株式会社富士通プログラム技研内
(74) 代理人 弁理士 林 恒徳 (外1名)

(54) 【発明の名称】 情報記憶装置及びその制御方法

(57) 【要約】

【課題】 記憶媒体に記録されたデータの機密性及びセキュリティを確保することができる情報記憶装置を提供する。

【解決手段】 記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体から第二の識別記号を獲得する識別記号獲得部と、第一の識別記号と第二の識別記号との対応関係に応じて、装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする情報記憶装置が提供される。例えば、制御部は、第一の識別記号と第二の識別記号とが一致しない場合に、装着された記憶媒体に対する情報の読み出し及び書き込みを禁止し、第一の識別記号と第二の識別記号が一致した場合は、装着された記憶媒体に対する情報の読み出し及び書き込みを許可する。このように、情報記憶装置に記憶された識別記号と異なる識別記号を有する記憶媒体は、その情報記憶装置での情報の読み書き不可することで、情報の機密性が確保される。



【特許請求の範囲】

【請求項1】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体の第二の識別記号を獲得する識別記号獲得部と、前記第一の識別記号と前記第二の識別記号との対応関係に応じて、前記装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする情報記憶装置。

【請求項2】請求項1において、前記制御部は、前記第一の識別記号と前記第二の識別記号とを比較した結果により、情報の読み出し及び／又は書き込みを禁止又は許可する判定を行うことを特徴とする情報記憶装置。

【請求項3】請求項1において、前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、前記制御部は、前記第一の識別記号と前記第二の識別記号との比較の結果と、前記読み出しアドレス情報に基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置。

【請求項4】請求項1又は3において、前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、前記制御部は、前記第一の識別記号と前記第二の識別記号との比較の結果と、該書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置。

【請求項5】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体の第二の識別記号を獲得する識別記号獲得部と、前記装着された記憶媒体に対して第一のアドレス情報が指定されると、前記装着された記憶媒体から第二のアドレス情報を獲得するアドレス情報獲得部と、前記第一の識別記号と前記第二の識別記号との対応関係と、前記第一のアドレス情報と前記第二のアドレス情報との対応関係に基づいて、前記装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする情報記憶装置。

【請求項6】請求項5において、前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、前記制御部は、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記読み出しアドレス情報に基づいて、情報の読み出しを許可又は禁

止することを特徴とする情報記憶装置。

【請求項7】請求項5又は6において、前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、前記制御部は、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置。

【請求項8】請求項1又は5において、前記装着された記憶媒体はパスワードを有し、前記制御部は、さらに、前記パスワードの判定により前記装着された記憶媒体の読み出し又は／及び書き込みのアクセス制御を行うことを特徴とする情報記憶装置。

【請求項9】請求項1又は5において、前記制御部は、指示された設定コマンドに基づいて、前記第一の識別記号を前記記憶部に記録する制御を行うことを特徴とする情報記憶装置。

【請求項10】請求項3又は6において、前記制御部は、指示された前記読み出しアドレス情報を有する所定の設定コマンドに基づいて、前記読み出しアドレス情報を前記装着された記憶媒体の所定領域に記録する制御を行うことを特徴とする情報記憶装置。

【請求項11】請求項4又は7において、前記制御部は、指示された前記書き込みアドレス情報を有する所定の設定コマンドに基づいて、前記書き込みアドレス情報を前記装着された記憶媒体の所定領域に記録する制御を行うことを特徴とする情報記憶装置。

【請求項12】請求項5において、前記制御部は、指示された前記第二のアドレス情報を有する所定の設定コマンドに基づいて、前記第二のアドレス情報を前記装着された記憶媒体の所定領域に記録する制御を行うことを特徴とする情報記憶装置。

【請求項13】請求項10乃至12のいずれかにおいて、前記制御部は、前記装着された記憶媒体の前記所定領域に記録される情報を暗号化することを特徴とする情報記憶装置。

【請求項14】請求項13において、前記制御部は、指示された暗号化情報を有する所定の設定コマンドに基づいて、前記装着された記憶媒体の前記所定領域に記録される情報を暗号化することを特徴とする情報記憶装置。

【請求項15】請求項10乃至12において、前記設定コマンドは、前記装着された記憶媒体の初期化コマンド又は設定のために設けられた特殊コマンドであることを特徴とする情報記憶装置。

【請求項16】請求項10乃至12において、前記制御部は、指示された解除コマンドに基づいて、前記所定領域を初期化することを特徴とする情報記憶装置。

置。

【請求項17】請求項10乃至12において、前記装着された記憶媒体の所定領域は、前記装着された記憶媒体のデータ領域以外に設定された媒体情報管理領域であることを特徴とする情報記憶装置。

【請求項18】請求項1乃至17のいずれかにおいて、前記記憶媒体は、磁気ディスク、フロッピーディスク、光ディスク、光磁気ディスク、相変化型光ディスクのうちのいずれかの可換型記憶媒体であることを特徴とする情報記憶装置。

【請求項19】請求項1乃至18のいずれかにおいて、前記第一及び第二の識別記号は、前記記憶媒体の製造番号であることを特徴とする情報記憶装置。

【請求項20】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置の制御方法において、記憶媒体の第一の識別記号を記憶するステップ前記第一の識別記号を獲得するステップと、装着された記憶媒体の第二の識別記号を獲得するステップと、

前記第一の識別記号と前記第二の識別記号との対応関係に応じて、前記装着された記憶媒体に対する情報の読み出し又は／及び書き込みのアクセス制御を行うステップとを有することを特徴とする情報記憶装置の制御方法。

【請求項21】請求項20において、前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号とを比較した結果により、情報の読み出し及び／又は書き込みを許可又は禁止する判定を行うことを特徴とする情報記憶装置の制御方法。

【請求項22】請求項20において、前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号との比較の結果と、前記読み出しアドレス情報とに基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置の制御方法。

【請求項23】請求項20又は22において、前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号との比較の結果と、該書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置の制御方法。

【請求項24】記憶媒体に対して第一のアドレス情報が指定されて情報の読み出し及び／又は書き込みを行う情報記憶装置の制御方法において、第一の記憶媒体の第一の識別記号を記憶するステップ前記第一の識別記号を獲得するステップと、装着された装着された記憶媒体の第二の識別記号を獲得するステップと、前記第一のアドレス情報を獲得するステップと、

前記記憶媒体に設定された第二のアドレス情報を獲得するステップと、

前記第一の識別記号と前記第二の識別記号との対応関係と、前記第一のアドレス情報と前記第二のアドレス情報との対応関係とに基づいて、前記装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行うステップとを有することを特徴とする情報記憶装置の制御方法。

【請求項25】請求項24において、前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記読み出しアドレス情報とに基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置の制御方法。

【請求項26】請求項24又は25において、前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置の制御方法。

【請求項27】請求項20又は24において、前記装着された記憶媒体はパスワードを有し、前記アクセス制御を行うステップは、さらに、前記パスワードの判定により前記装着された記憶媒体の読み出し及び／又は書き込みのアクセス制御を行うことを特徴とする情報記憶装置の制御方法。

【請求項28】請求項22又は25において、前記読み出しアドレス情報を前記装着された記憶媒体の所定領域に記録するステップをさらに有することを特徴とする情報記憶装置の制御方法。

【請求項29】請求項23又は26において、前記書き込みアドレス情報を前記装着された記憶媒体の所定領域に記録するステップをさらに有することを特徴とする情報記憶装置の制御方法。

【請求項30】請求項24において、前記第二のアドレス情報を前記装着された記憶媒体の所定領域に記録するステップをさらに有することを特徴とする情報記憶装置の制御方法。

【請求項31】請求項27乃至30のいずれかにおいて、前記装着された記憶媒体の前記所定領域に記録される情報を暗号化するステップをさらに有することを特徴とする情報記憶装置の制御方法。

【請求項32】請求項27乃至30において、

前記記録するステップは、前記装着された記憶媒体の初期化コマンド又は記録のために設けられた特殊コマンドに基づいて行われることを特徴とする情報記憶装置の制御方法。

【請求項33】請求項27乃至30において、前記所定領域の設定を解除する場合、前記所定領域を初期化することを特徴とする情報記憶装置の制御方法。

【請求項34】請求項27乃至30において、前記装着された記憶媒体の所定領域は、前記記憶媒体のデータ領域以外に設定された媒体情報管理領域であることを特徴とする情報記憶装置の制御方法。

【請求項35】請求項20乃至34のいずれかにおいて、前記記憶媒体は、磁気ディスク、フロッピーディスク、光ディスク、光磁気ディスク、相変化型光ディスクのうちのいずれかの可換型記憶媒体であることを特徴とする情報記憶装置の制御方法。

【請求項36】請求項20乃至35のいずれかにおいて、前記第一及び第二の識別記号は、前記記憶媒体の製造番号であることを特徴とする情報記憶装置の制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、光磁気ディスクなどの記憶媒体にデータ（情報）を記録する情報記憶装置に係り、特に、記録されたデータの機密性及びセキュリティを確保することができる情報記憶装置に関する。

【0002】

【従来の技術】一般に、光磁気ディスク（MO）などのようなデータの書き込みが可能な記憶媒体は、所定のデータ読み出し及び書き込みを行う情報記憶装置（以下、記憶装置という）に着脱可能となっており、装着された際、記憶装置によって、データの読み書きが行われる。また、記憶装置は、例えば、SCSIケーブルなどで接続されたパーソナルコンピュータのような上位装置からのコマンドによって制御される。

【0003】このような記憶媒体において、従来、互換性重視の観点から、データを書き込んだ記憶装置と異なる別の記憶装置によっても、そのデータの読み出し及び書き込みが可能である。

【0004】図18は、従来の記憶装置におけるデータの読み書きフローチャートである。ステップS1において、媒体が記憶装置に挿入されると、ステップS2において、媒体がロードされる。即ち、媒体は、記憶装置の所定位置に設置され、規定回転数で回転する。そして、ステップS3において、媒体の構成や記憶容量などの所定の媒体情報が読み出された後、この媒体情報に対応した動作や処理によってデータの読み出し及び書き込みが可能となる（ステップS4）。

【0005】

【発明が解決しようとする課題】従って、記憶媒体さえ入手すれば、それに記録されている例えば顧客データベースや設計情報などの機密情報を容易に盗用又は改ざんすることができるという問題が生じていた。

【0006】そこで、本発明の目的は、上記問題点に鑑み、記憶媒体に記録されたデータの機密性及びセキュリティを確保することができる情報記憶装置を提供することである。

【0007】

【課題を解決するための手段】上記目的を達成するための本発明の情報記憶装置は、記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体から第二の識別記号を獲得する識別記号獲得部と、第一の識別記号と第二の識別記号との対応関係に応じて、第二の記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする。

【0008】例えば、制御部は、第一の識別記号と第二の識別記号とが一致しない場合に、装着された記憶媒体に対する情報の読み出し及び書き込みを禁止し、第一の識別記号と第二の識別記号が一致した場合は、装着された記憶媒体に対する情報の読み出し及び書き込みを許可する。

【0009】このように、情報記憶装置に書き込まれた識別記号と異なる識別記号を有する記憶媒体は、その情報記憶装置での情報の読み書き不可とすることで、情報の機密性が確保される。

【0010】また、装着された記憶媒体の所定領域は、情報の読み出しを制御する読み出しアドレス情報又は書き込みを制御する書き込みアドレス情報を有し、制御部は、第一の識別記号と第二の識別記号との比較の結果と、それぞれ読み出しアドレス情報又は書き込みアドレス情報とに基づいて、情報の読み出しを許可又は禁止するようにしてもよい。

【0011】さらに、上記目的を達成するための本発明の情報記憶装置は、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体から第二の識別記号を獲得する識別記号獲得部と、装着された記憶媒体に対して第一のアドレス情報が指定されると、装着された記憶媒体から第二のアドレス情報を獲得するアドレス情報獲得部と、第一の識別記号と第二の識別記号との対応関係と、第一のアドレス情報と第二のアドレス情報との対応関係とに基づいて、装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする。

【0012】これにより、装着された記憶媒体に記録された複数の情報毎にセキュリティを設定することができる。

【0013】また、装着された記憶媒体の所定領域は、

情報の読み出しを制御する読み出しアドレス情報又は書き込みアドレス情報を有し、制御部は、第一の識別記号と第二の識別記号が一致し、且つ第二のアドレス情報が第一のアドレス情報に含まれる場合、それぞれ読み出しアドレス情報又は書き込みアドレス情報に基づいて、情報の読み出しを許可又は禁止するようにしてもよい。

【0014】さらに、上述のような構成の情報記憶装置において、制御部は、情報記憶装置と接続された情報記憶装置の制御装置から送られる所定の設定コマンドに基づいて、読み出しアドレス情報、書き込みアドレス情報又は第二のアドレス情報を、装着された記憶媒体の所定領域に記録する。そして、所定の設定コマンドは、例えば、スキャジーインターフェースにおけるフォーマットコマンド又はベンダーユニークコマンドである。さらに、制御部は、上記制御装置から送られる所定の解除コマンドに基づいて、所定領域を初期化できることが好ましい。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について説明する。しかしながら、本発明の技術的範囲がこの実施の形態に限定されるものではない。なお、図において同一又は類似のものには同一の参照数字又は参照記号を付して説明する。

【0016】本発明の実施の形態においては、データが記録される媒体として光磁気ディスク(MO)に基づいた説明を行うが、記憶媒体はこれに限定されるものではなく、例えば磁気ディスク、フロッピーディスク、光ディスク、相変化型光ディスクのような他の可換型記憶媒体であってもよい。

【0017】図1は、本発明の実施の形態における光磁気ディスク装置の概略ブロック構成図である。図1によれば、光磁気ディスク装置1は、上位装置であるパーソナルコンピュータ2とSCSIインターフェースを介して接続されている。

【0018】そして、光磁気ディスク装置1は、光磁気ディスクに対する書き込み及び読み出しを行う機構制御部10を有し、さらに、本発明を実行するためのソフトウェアが格納されたファームウェアを有する光磁気ディスク制御部(ODC)11を備えた制御回路部を備える。

【0019】制御回路部は、さらに、光磁気ディスク装置1の全体制御を行うMPU12、読み取り/書き込み用バッファメモリであるD-RAM13、位置決め制御を行うDSP14、書き込みデータ増幅回路14、読み取りデータ増幅回路16、AGC増幅回路17、ヘッド駆動用電力増幅回路18及びディスク回転モータ制御回路19を有する。

【0020】機構制御部10は、ヘッドセンサ100、データ読み取り/書き込み用レーザダイオード101、ヘッドの傾きなどを検出するディテクタ102を有す

る。さらに、機構制御部10は、ヘッド駆動用電力増幅回路18により制御されるフォーカスアクチュエータ回路103、トラックアクチュエータ回路104、ディスク取り出し(イジェクト)モータ105及びヘッド駆動用ボイスコイルモータ106を有し、また、モータ制御回路19により回転制御され、ディスクを回転するスピンドルモータ107を備える。

【0021】一方、パーソナルコンピュータ2のキーボード3から入力されるオペレータの指示に対応し、コンピュータ2から光磁気ディスク制御部(ODC)11に対してSCSIコマンドが送信されて、データの書き込み/読み出し制御が行われる。また、コンピュータ2には、書き込みデータ及び読み出しデータを表示するディスプレイ4が接続される。

【0022】光磁気ディスク制御部(ODC)11は、フラッシュROMで構成されるファームウェアを有し、コンピュータ2から送られるSCSIコマンドを解析する機能を有する。さらに、SCSIコマンドに対応して、MPU12と協働して、機構制御部10に対して書き込み/読み出し制御を行う機能を有する。

【0023】なお、本発明の適用は、SCSIコマンド系に限定されず、ATA/ATAPI/SASIなどの他のコマンド体系でも適用できることはいうまでもない。

【0024】図2は、光磁気ディスク(MO)のディスクフォーマットのレイアウト例であって、3.5インチ光磁気ディスクカートリッジに関するISO規格により決められた媒体の領域区分である。図2に示されるように、円盤状のMOの中心から半径23.72mmから半径41.00mmの範囲が、使用者がデータ書き込み可能なデータ領域である。そして、その半径方向の内側と外側は、媒体の種類及び構成などの各種媒体情報が記録される媒体情報管理領域である。

【0025】本発明の実施の形態においては、この媒体情報管理領域にセキュリティ領域が新たに設けられ、そのセキュリティ領域にあらかじめ記録されたセキュリティ情報である媒体の製造番号のような識別記号が、光磁気ディスク装置(以下、記憶装置という)に書き込まれる。または、例えば図2におけるインナーテストゾーン(Inner Test Zone)及びアウトertestゾーン(Outer Test Zone)のマニファクチャラゾーン(for manufactures)やバッファゾーン(Buffer Zone)などをセキュリティ領域として代用してもよい。

【0026】そして、あらかじめ識別記号であるセキュリティ情報が記録された光磁気ディスク(以下、媒体という)が、ある記憶装置に挿入されたとき、その記憶装置に書き込まれた識別記号と媒体にあらかじめ記録された識別記号との対応関係に応じて、データの読み書きを制御する。例えば、両識別記号が一致した場合のみ、データの読み書きを可能にする。即ち、媒体に書き込まれ

た識別記号と異なる識別記号を有する記憶装置では、その媒体におけるデータの読み書き不可とすることで、データの機密性が確保される。

【0027】また、識別記号の記憶装置への書き込み処理は、上位装置からのセキュリティ設定コマンドに基づいて記憶装置の上記光磁気ディスク制御部（ODC）11において行われる。

【0028】図3は、識別記号の記憶装置への書き込み処理フローチャートを示す図である。図3によれば、ステップS11において、記憶装置がセキュリティ設定コマンドを受けると、ステップS12において、記憶装置に既にセキュリティ情報が書き込まれているか否かが判断される。このとき、すでに書き込まれている場合、即ち既にセキュリティが設定されている場合は、ステップS13において、書き込まれたセキュリティ情報の識別記号と、挿入されている記憶媒体の識別記号が比較される。そして、両識別記号が一致しない場合は、挿入された記憶媒体のセキュリティ確保のため、セキュリティ設定コマンドは異常終了する（ステップS19）。一方、セキュリティ情報が書き込まれていない初期状態である場合は、ステップS14に進み、挿入されている記憶媒体の識別記号が読み出される。そして、ステップS15において、その識別記号が記憶装置1のODC11の所定記憶領域に書き込まれる。また、後述するように、記憶媒体に記憶されているデータの一部分のみセキュリティが設定される場合は、ステップS16において、セキュリティが設定されるデータのアドレス情報が記憶媒体のセキュリティ領域に書き込まれる。そして、ステップS17において、記憶装置1は、セキュリティ設定コマンドで指定されたモードに変更され、セキュリティ設定コマンドは正常終了する（ステップS18）。

【0029】図4は、パーソナルコンピュータ2から記憶装置1に送られるセキュリティ設定コマンドのCDB（コマンド・ディスクリプタ・ブロック）の例を示す図である。図4のセキュリティ設定コマンドは、SCSIインターフェースにおけるベンダーユニーク（Vendor Unique）コマンドを使用して設定される。そして、上述のように、媒体上に書き込まれた識別記号と挿入されている記憶装置の識別記号が一致したときのみ媒体にアクセス可能とするセキュリティ設定情報が、セキュリティ設定コマンドのセキュリティレベルに設定される。

【0030】また、上記セキュリティレベルは、ベンダーユニークコマンドを利用したセキュリティ設定コマンドに代わって、通常のフォーマット（Format）コマンドに設定されてもよい。図5は、SCSIコマンドにおいて、上記セキュリティレベルが設定されたフォーマットコマンドのCDBの例を示す図である。

【0031】図6は、上述のような記憶装置における本発明の第一の実施の形態であるセキュリティ処理のフローチャートである。以下に説明するセキュリティ処理

は、記憶装置1の光磁気制御部（ODC）11において実行される。

【0032】図6によれば、ステップS101において、媒体が記憶装置に挿入されると、ステップS102において、媒体がロードされる。即ち、媒体は、記憶装置の所定位置に設置され、規定回転数で回転する。そして、ステップS103において、媒体における上記媒体情報管理領域上の情報が読み出され、さらに、ステップS104において、その中の上記セキュリティ領域に書き込まれたセキュリティ情報（識別記号）が読み出される。

【0033】ステップS105において、上記セキュリティ領域の情報が初期状態であるか否かが判断される。そして、上記セキュリティ領域が初期状態である場合、即ち、上記セキュリティ領域に識別記号が書き込まれていない場合、セキュリティが設定されていないものとして、ステップS108に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。

【0034】一方、ステップS105において、セキュリティ領域に識別記号が書き込まれている場合、即ち、セキュリティが設定されている場合、ステップS106において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。

【0035】そして、両者が一致する場合は、セキュリティが解除され、ステップS108に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。

【0036】一方、ステップS106において、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される（ステップS107）。

【0037】このように、本発明の実施の形態においては、媒体上の媒体情報管理領域に、セキュリティ情報が書き込まれるセキュリティ領域が設けられる。そして、媒体が記憶装置にロードされた際、ロードされた記憶媒体の識別記号（セキュリティ情報）と、媒体に書き込まれた識別記号が一致しない場合は、データの読み書きを禁止することで、媒体が盗用された場合であっても、媒体に書き込まれたデータの機密性を確保することができる。

【0038】ところで、上述の第一の実施の形態においては、媒体にセキュリティが設定された状態であっても、例えばその媒体を盗用した他人が媒体に書き込まれた識別記号と同じ識別記号を有する記憶装置を用いることによって、その媒体のデータの読み書きが可能である。

【0039】そこで、媒体に書き込まれた識別記号と、その媒体がロードされた記憶装置の識別記号とが一致する場合であっても、データの読み書きを制限するセキュリティ機能が設定されることが好ましい。

【0040】そのために、上記セキュリティ設定コマンド(図4)又はセキュリティレベルが設定されたフォーマットコマンド(図5)で指定されるパラメータのパラメータヘッダに読み出しアドレス情報と書き込みアドレス情報が設定される。図7は、上記各コマンドで指定されるパラメータの構成例である。パラメータは、図7

(a)に示されるパラメータヘッドと、図7(b)に示されるレベルディスクリプタから構成される。そして、上記各アドレス情報は、図7(a)のパラメータヘッドに設定される。なお、図7(b)に示すレベルディスクリプタは、2バイト長のヘッダとそれに続くパラメタフィールドから構成される。そして、パラメタフィールドは、さらに機能属性ごとにページと呼ばれる単位に分類される。

【0041】例えば、読み出しアドレス情報が設定されている場合は、識別記号が一致した場合であっても、データの読み出しが禁止される。また、読み出しアドレス情報が設定されていない場合は、データの読み出しは許可される。

【0042】さらに、書き込みアドレス情報が設定されている場合は、識別記号が一致した場合であっても、データの書き込みが禁止される。また、書き込みアドレス情報が設定されていない場合は、データの書き込みは許可される。これら読み出しアドレス情報及び書き込みアドレス情報は、記憶装置の識別記号がセキュリティ領域に書き込まれる際に、同時にセキュリティ領域に書き込まれる。

【0043】なお、読み出しアドレス情報又は書き込みアドレス情報が設定されていると、識別記号が一致した場合であっても、データの読み出し又は書き込みができなくなり不都合である。従って、読み出しアドレス情報又は書き込みアドレス情報が設定される場合は、同時に所定パスワードが設定され、各アドレス情報が設定されている場合であっても、パスワードが入力された場合は、読み出し又は書き込みが可能となるようにすることが好ましい。さらに、各アドレス情報の設定の有無に関わらず、所定パスワードが設定され、識別記号とパスワードの両方が一致した場合に、読み書きを許可することにより、セキュリティを二重に設定することが可能となり、よりデータの機密性を向上させることができる。

【0044】また、パスワードは、上記パラメータのレベルディスクリプタに設定される。図8(a)は、レベルディスクリプタのパラメタフィールド(図7(b)参照)におけるパスワードのページを示す図である。そして、このパスワードは、セキュリティ設定の際に、アドレス情報とともに、媒体のセキュリティ領域に書き込まれる。なお、図8(b)は、レベルディスクリプタのパラメタフィールドにおける後述する論理ブロックアドレス(LBA)の指定ページを示す図である。

【0045】図9は、本発明の第二の実施の形態におけ

るセキュリティ処理のフローチャートである。本第二の実施の形態においては、上述のパラメータヘッダに読み出しアドレス情報が設定されていた場合である。図9においては、ステップS201乃至ステップS205は、上記図6におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【0046】ステップS205において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS211に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS205において、セキュリティ情報が設定されている場合、ステップS206において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される(ステップS207)。

【0047】一方、両者が一致する場合は、ステップS208に進み、読み出しアドレス情報に基づいて、読み出し可否の判断が行われる。読み出しアドレス情報が設定されていない場合は、ステップS209に進み、データの読み出しが許可されるが、データの書き込みは禁止される。即ち、保存されているデータを読み込んで、その内容を見ることはできるが、そのデータの変改などの書き込みはできない。また、読み出しアドレス情報が設定されている場合は、ステップS210に進み、読み出し、書き込みともに禁止される。

【0048】図10は、本発明の第三の実施の形態におけるセキュリティ処理のフローチャートである。本第三の実施の形態においては、上述のパラメータヘッダに上記書き込みアドレス情報が設定されていた場合である。図10においては、ステップS301乃至ステップS305は、上記図6におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【0049】ステップS305において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS311に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS305において、セキュリティが設定されている場合、ステップS306において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される(ステップS307)。

【0050】一方、両者が一致する場合は、ステップS308に進み、書き込みアドレス情報に基づいて、読み出し可否の判断が行われる。読み出しアドレス情報が設定されていない場合は、ステップS309に進み、データの書き込みが許可されるが、データの読み出し書き込みは禁止

される。即ち、新たなデータを作成することはできるが、保存されているデータを読み込むことはできない。また、読み出しアドレス情報が設定されている場合は、ステップS310に進み、読み出し及び書き込みともに禁止される。

【0051】図11は、本発明の第四の実施の形態におけるセキュリティ処理のフローチャートである。本第四の実施の形態においては、上述のパラメータヘッダに上記読み出しアドレス情報と書き込みアドレス情報がともに設定されていた場合である。

【0052】ステップS405において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS415に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS405において、セキュリティ情報が設定されている場合、ステップS406において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される（ステップS407）。

【0053】一方、両者が一致する場合は、ステップS408に進み、まず、読み出しアドレス情報に基づいた読み出し可否の判断が行われる。そして、読み出しアドレス情報が設定されていない場合は、ステップS409に進み、次に書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップS410に示すように、データの読み出しと書き込みともに許可される。一方、ステップS409において、書き込みアドレス情報が設定されている場合は、ステップS411に示されるように、データの読み出しが許可されるが、データの書き込みは禁止される。

【0054】また、ステップS408において、読み出しアドレス情報が設定されている場合は、ステップS412に進み、ステップS409同様に、書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップS413に示すように、データの書き込みは許可されるが、データの読み出しは禁止される。一方、ステップS412において、書き込みアドレス情報が設定されている場合は、ステップS414に示されるように、データの読み出しと書き込みともに禁止される。

【0055】上述の各実施の形態におけるデータの読み出しは、その媒体に保存されているデータ全てが対象である。しかしながら、媒体に複数のデータが保存されている場合に、その一部にのみセキュリティを設定したい場合が想定される。

【0056】そのために、媒体にセキュリティ設定が行われるとき、上記図7のパラメータのレベルディスクリ

プタにセキュリティを設定したいデータの論理ブロックアドレス（LBA）が指定される。さらに詳しくは、セキュリティを設定するデータを指定するためのLBA指定ページがレベルディスクリプタのパラメータフィールドに設定される（前述の図8（b）参照）。そして、図8（b）に示されるように、セキュリティを設定する1つデータのLBA（セキュリティLBA）が例えば3バイト長で指定される。このセキュリティLBAの情報は、記憶装置の識別記号がセキュリティ領域に書き込まれる際に、同時にセキュリティ領域に書き込まれる。

【0057】図12は、本発明の第五の実施の形態におけるセキュリティ処理のフローチャートである。本第五の実施の形態は、上述の第二の実施の形態と同様に、読み出しアドレス情報が設定されている場合に、さらに、セキュリティLBAが設定されている場合である。図12においては、ステップS501乃至ステップS505は、上記図6におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【0058】ステップS505において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS516に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS505において、セキュリティ情報が設定されている場合、ステップS506において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、ステップS507において、セキュリティ領域にセキュリティLBAの指定の有無が判断される。そして、セキュリティLBAの指定がない場合は、媒体全体の読み出し及び書き込みが禁止される（ステップS508）。

【0059】一方、ステップS507において、セキュリティLBAの指定がある場合は、ステップS509において、アクセスしているデータのLBAが、セキュリティLBAに含まれているか否かが判断される。含まれていれば、ステップS510に進み、そのデータの読み出し及びデータの書き込みが禁止される。

【0060】また、含まれていないならば、ステップS511に進み、そのデータの読み出し及び書き込みが許可される。

【0061】さらに、ステップS506において、両者の識別記号が一致する場合も、ステップS512において、アクセスしているデータのLBAが、セキュリティLBAに含まれているか否かが判断される。含まれていれば、ステップS513に進み、読み出しアドレス情報に基づいた読み出し可否の判断が行われる。

【0062】そして、読み出しアドレス情報が設定されていない場合は、ステップS514に進み、データの読み出しが許可されるが、データの書き込みは禁止される。即ち、保存されているデータを読み込んで、その内容を見

ることはできるが、そのデータの改変などの書き込みはできない。また、読み出しアドレス情報が設定されている場合は、ステップS515に進み、読み出し、書き込みともに禁止される。

【0063】また、ステップS512において、アクセスしているデータのLBAがセキュリティLBAが含まれていないならば、ステップS516に進み、データの読み出し及び書き込みともに許可される。

【0064】図13は、本発明の第六の実施の形態におけるセキュリティ処理のフローチャートである。本第六の実施の形態は、上述の第三の実施の形態と同様に、書き込みアドレス情報が設定されている場合に、さらに、セキュリティLBAが設定されている場合である。図13においては、ステップS601乃至ステップS605は、上記図6におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【0065】ステップS605において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS616に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS605において、セキュリティ情報が設定されている場合、ステップS606において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、ステップS607において、セキュリティ領域にセキュリティLBAの指定の有無が判断される。そして、セキュリティLBAの指定がない場合は、媒体全体の読み出し及び書き込みが禁止される（ステップS608）。

【0066】一方、ステップS607において、セキュリティLBAの指定がある場合は、ステップS609において、アクセスしているデータのLBAが、セキュリティLBAに含まれているか否かが判断される。含まれていれば、ステップS610に進み、そのデータの読み出し及びデータの書き込みが禁止される。

【0067】また、含まれていないならば、ステップS611に進み、そのデータの読み出し及び書き込みが許可される。

【0068】さらに、ステップS606において、両者の識別記号が一致する場合も、ステップS612において、アクセスしているデータのLBAが、セキュリティLBAに含まれているか否かが判断される。含まれていれば、ステップS613に進み、書き込みアドレス情報に基づいた書き込み可否の判断が行われる。

【0069】そして、書き込みアドレス情報が設定されていない場合は、ステップS614に進み、データの書き込みが許可されるが、データの読み出しは禁止される。即ち、新たなデータの作成は許可されるが、保存されているデータを見ることはできない。また、書き込みアドレス情報が設定されている場合は、ステップS615に進み、

読み出し、書き込みともに禁止される。

【0070】また、ステップS612において、アクセスしているデータのLBAがセキュリティLBAが含まれていないならば、ステップS616に進み、データの読み出し及び書き込みともに許可される。

【0071】図14は、本発明の第七の実施の形態におけるセキュリティ処理のフローチャートである。本第七の実施の形態は、上述の第三の実施の形態と同様に、読み出しアドレス情報及び書き込みアドレス情報が設定されている場合に、さらに、セキュリティLBAが設定されている場合である。図14においては、ステップS701乃至ステップS705は、上記図6におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【0072】ステップS705において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS720に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS705において、セキュリティ情報が設定されている場合、ステップS506において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、ステップS707において、セキュリティ領域にセキュリティLBAの指定の有無が判断される。そして、セキュリティLBAの指定がない場合は、媒体全体の読み出し及び書き込みが禁止される（ステップS708）。

【0073】一方、ステップS707において、セキュリティLBAの指定がある場合は、ステップS709において、アクセスしているデータのLBAが、セキュリティLBAに含まれているか否かが判断される。含まれていれば、ステップS710に進み、そのデータの読み出し及びデータの書き込みが禁止される。

【0074】また、アクセスしているデータのLBAが、セキュリティLBAに含まれていないならば、ステップS711に進み、そのデータの読み出し及び書き込みが許可される。

【0075】さらに、ステップS706において、両者の識別記号が一致する場合も、ステップS512において、アクセスしているデータのLBAが、セキュリティLBAに含まれているか否かが判断される。含まれていれば、ステップS713に進み、まず、読み出しアドレス情報に基づいた読み出し可否の判断が行われる。そして、読み出しアドレス情報が設定されていない場合は、ステップS714に進み、次に書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップS715に示すように、データの読み出しと書き込みともに許可される。一方、ステップS715において、書き込みアドレス情報が設定されている場合は、ステップS716に示されるように、

データの読み出しが許可されるが、データの書き込みは禁止される。

【0076】また、ステップS713において、読み出しアドレス情報が設定されている場合は、ステップS717に進み、ステップS714同様に、書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップS718に示すように、データの書き込みは許可されるが、データの読み出しは禁止される。一方、ステップS717において、書き込みアドレス情報が設定されている場合は、ステップS719に示されるように、データの読み出しと書き込みともに禁止される。また、ステップS712において、アクセスしているデータのLBAがセキュリティLBAが含まれていないならば、ステップS720に進み、データの読み出し及び書き込みともに許可される。

【0077】そして、図15は、上述した様々なセキュリティ処理が実行されるセキュリティ設定状態を解除するセキュリティ解除の処理フローチャートである。

【0078】まず、ステップS801において、セキュリティ解除コマンドをコンピュータ2より記憶装置に送る。セキュリティ解除コマンドは、上記セキュリティ設定コマンドと同様に、SCSIコマンドのベンダーユニークを利用して構成される。

【0079】そして、ステップS802において、セキュリティ領域のアドレス情報が読み出され、ステップS803において、セキュリティ領域にセキュリティ情報の有無が確認される。セキュリティ情報が書き込まれている場合は、ステップS804に進み、セキュリティ情報に含まれる識別記号と、媒体が挿入されている記憶装置の識別記号とが比較される。一致する場合は、セキュリティ領域には、所定の初期値が書き込まれ、初期状態に戻される（初期化される）（ステップS805）。

【0080】一方、識別記号が一致しない場合、若しくは元々セキュリティ領域にセキュリティ情報が書き込まれていない場合は、セキュリティ解除は行われない。

【0081】なお、上記のフローチャートには図示されないが、セキュリティ情報がパスワードを有している場合は、パスワードを入力するステップが設けられ、セキュリティ情報に含まれるパスワードと、入力されたパスワードが一致した場合のみ、セキュリティ解除が実行されるようにしてもよい。

【0082】上述した各本発明の実施の形態において、セキュリティ領域に書き込まれるセキュリティ情報（識別記号、アドレス情報、パスワードなど）は、さらに、機密性を高めるために暗号化されて書き込まれてもよい。この場合は、セキュリティ設定コマンドには、暗号化を指示する所定の暗号化情報が追加され、その暗号化情報に基づいて暗号化されたセキュリティ情報がセキュリティ領域に書き込まれる。

【0083】図16は、セキュリティ情報が暗号化され

ている場合における媒体ロード時の処理例のフローチャートである。図16において、ステップS901において、記憶装置に媒体が挿入されると、ステップS902において、媒体ロードが開始される。そして、ステップS903において、媒体管理情報が読み出され、さらに、ステップS904において、その中におけるセキュリティ情報の有無が判断される。

【0084】ステップS904において、セキュリティ情報がない場合は、ステップS909に進み、媒体におけるデータの読み出し及び書き込みが可能となる。

【0085】一方、ステップS904において、セキュリティ情報がある場合は、次に、ステップS905において、セキュリティ情報が暗号化されているか否かが判断される。そして、ステップS906において、暗号化されている場合は、セキュリティ情報の暗号化が解除される。

【0086】そして、ステップS907において、セキュリティ情報が有する識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。両者が一致する場合は、セキュリティが解除され、ステップS909に進み、媒体におけるデータの読み出し及び書き込みが可能となる。

【0087】一方、ステップS907において、両者が一致しない場合は、セキュリティが解除されず、媒体におけるデータの読み出し及び書き込みが不可能となる（ステップS908）。

【0088】さらに、図17は、図16において、セキュリティ情報が、さらにパスワードを有する場合の媒体ロード時の処理例のフローチャートである。図17によれば、図16のフローチャートにステップS910が追加される。即ち、ステップS906において、暗号化が解除されると、入力されたパスワードとセキュリティ情報が有するパスワードとが比較される。そして、両者が一致しない場合は、セキュリティが解除されず、媒体におけるデータの読み出し及び書き込みが不可能となる（ステップS908）。

【0089】一方、両者が一致する場合は、ステップS907に進み、さらに、上述した識別記号の比較が行われる。

【0090】このとき、ステップS907とステップS910、即ち、パスワードの比較と識別記号の比較の順番は、反対であってもかまわない。そして、パスワードの比較のステップの設定、及び識別記号の比較のステップは、ユーザ又は記憶装置の製造業者若しくは販売業者によって任意に設定可能であって、その設定も任意に変更可能である。

【0091】また、上記セキュリティ情報の暗号化は、例えば、DESアルゴリズムや単純なビット並べ替えなどによって行われる。さらに、上記セキュリティ情報は、例えば、ASCII、JIS、EDICIBIC、ECUコードなどに変換されて上記セキュリティ領域に書き込まれてもよ

い。

【0092】さらに、上述した各本発明の実施の形態においては、識別記号が一致した場合に読み出し又は書き込みを許可する制御が行われるが、不一致となった場合に許可するような制御が行われてもよい。

【0093】

【発明の効果】以上説明したとおり、本発明によれば、光磁気ディスクのような記憶媒体の媒体情報管理領域に設けられたセキュリティ領域にあらかじめ記録された識別記号（セキュリティ情報）が、情報記憶装置固有の識別記号として書き込まれる。そして、このような記憶媒体が情報記憶装置に挿入された際、記憶媒体に記録された識別記号と、挿入された情報記憶装置の識別記号が一致しないときは、記憶媒体のデータにアクセス不可にすることで、データの機密性を確保することができる。このように、情報記憶装置に記憶された識別記号と異なる識別記号を有する記憶媒体は、その情報記憶装置での情報の読み書き不可とすることで、情報の機密性が確保される。

【図面の簡単な説明】

【図1】本発明の実施の形態におけるデータ記憶装置のブロック構成図である。

【図2】光磁気ディスクのディスクフォーマットのレイアウト例である。

【図3】記憶装置への識別記号の書き込み処理フローチャートを示す図である。

【図4】ベンダーユニークコマンドを使用したセキュリティ設定コマンドのCDBの構成例である。

【図5】セキュリティレベルが設定されたフォーマットコマンドのCDBの構成例である。

【図6】本発明の第一の実施の形態におけるセキュリティ

処理フローチャートである。

【図7】パラメータのパラメータヘッダ及びレベルディスクリプタの構成例である。

【図8】レベルディスクリプタのパラメータフィールドの構成例である。

【図9】本発明の第二の実施の形態におけるセキュリティ処理フローチャートである。

【図10】本発明の第三の実施の形態におけるセキュリティ処理フローチャートである。

【図11】本発明の第四の実施の形態におけるセキュリティ処理フローチャートである。

【図12】本発明の第五の実施の形態におけるセキュリティ処理フローチャートである。

【図13】本発明の第六の実施の形態におけるセキュリティ処理フローチャートである。

【図14】本発明の第七の実施の形態におけるセキュリティ処理フローチャートである。

【図15】セキュリティ解除の処理フローチャートである。

【図16】セキュリティ情報が暗号化されている場合における媒体ロード時の処理例のフローチャートである。

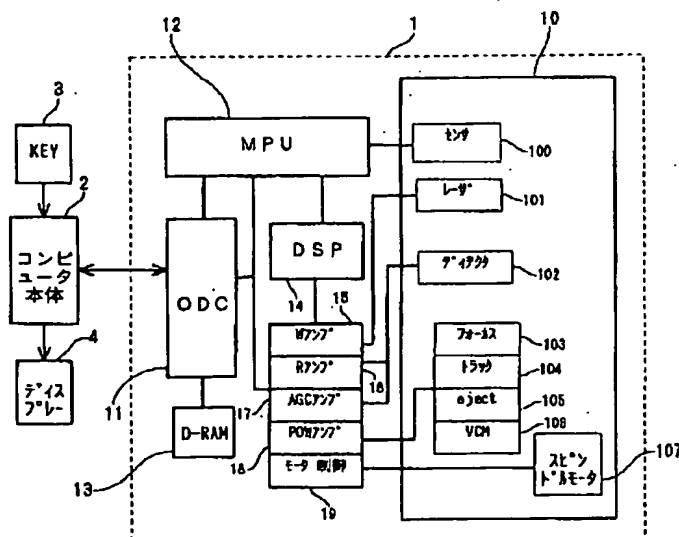
【図17】セキュリティ情報が暗号化され、さらに、パスワードが設定されている場合における媒体ロード時の処理例のフローチャートである。

【図18】従来における媒体へのアクセス処理フローチャートである。

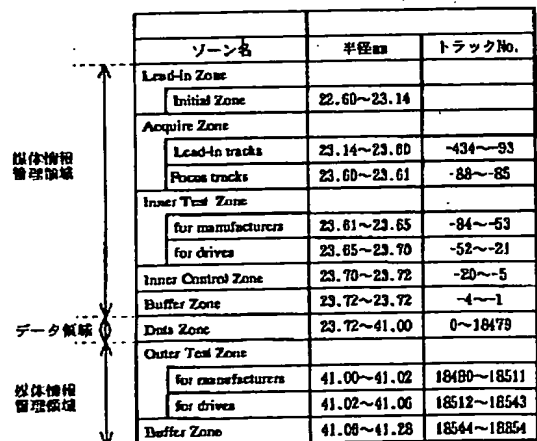
【符号の説明】

- 1 データ記憶装置
- 2 パーソナルコンピュータ
- 10 機構制御部
- 11 光磁気ディスク制御部

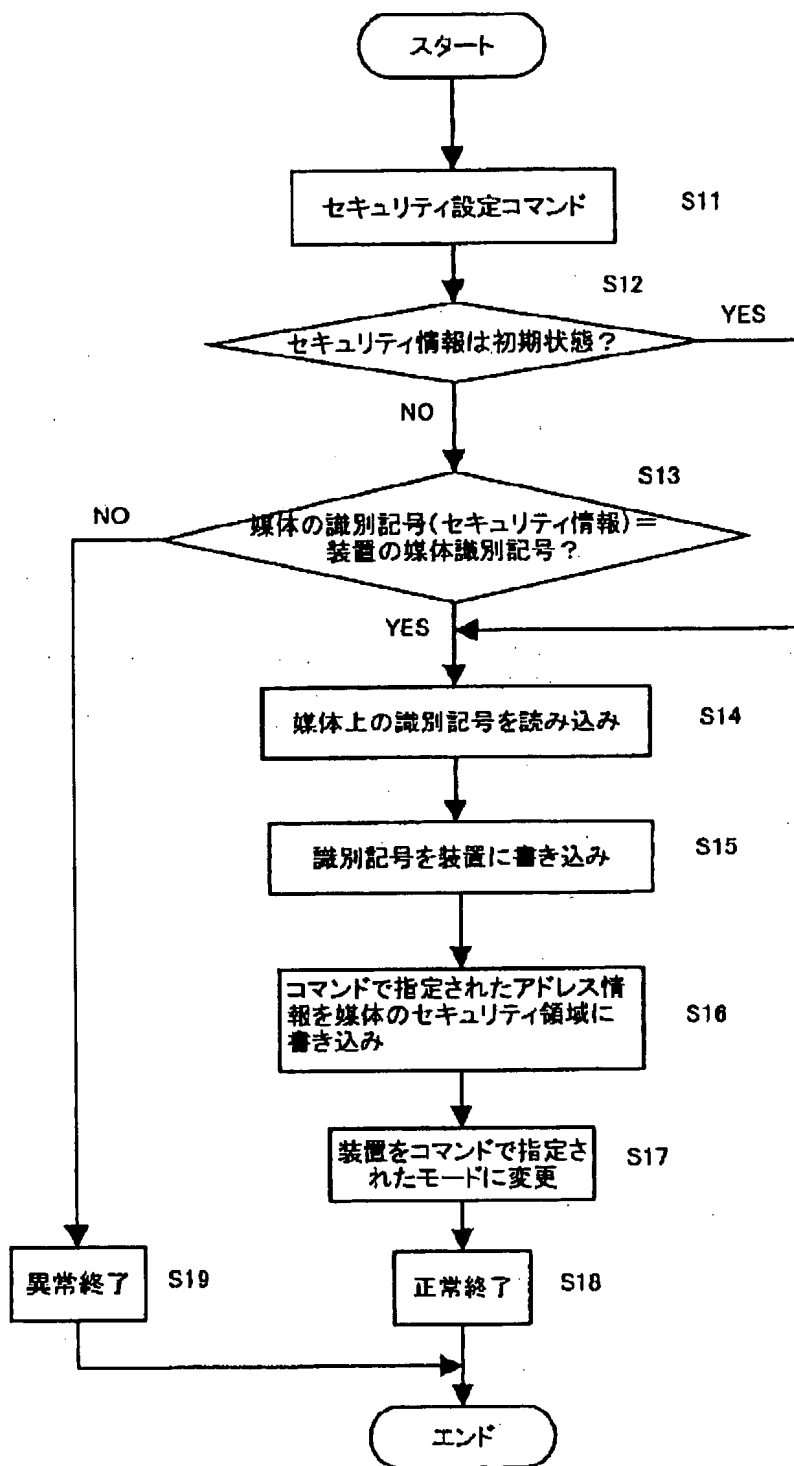
【図1】



【図2】



【図3】



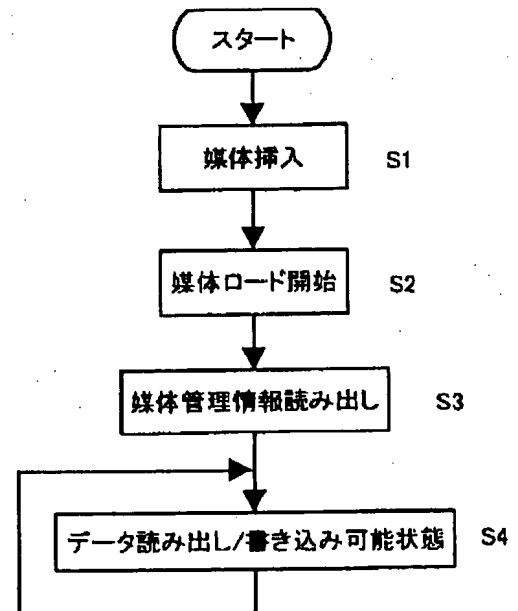
【図4】

		Bit								
		7	6	5	4	3	2	1	0	
Byte	00	0	0	0	0	0	0	1	0	0
	01	LUN			FMT DATA		CMP LIST		DEFECT LIST FORMAT	
	02	セキュリティレベル								
	03	INTERLEAVE								
	04	INTERLEAVE								
	05	0	0	0	0	0	0	0	Flag	Link

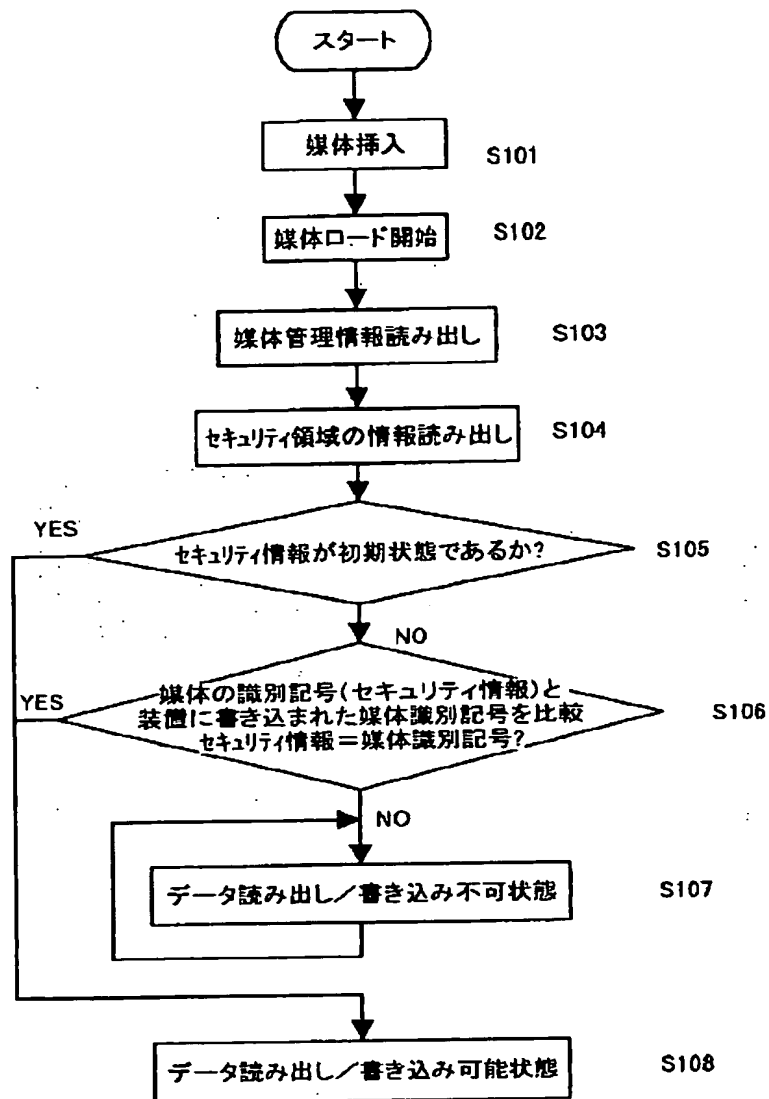
【図5】

Byte	Bit							
	7	6	5	4	3	2	1	0
00	1	1	1	0	0	0	0	0
01	LUN			0	0	0	0	0
02	セキュリティレベル							
03	X'00'							
04	パラメタリスト長							
05	0	0	0	0	0	0	Flag	Link

【図18】



【図6】



【図7】

(a)								
Bit	7	6	5	4	3	2	1	0
Byte								
0	X' 00'							
1	X' 00'							
2	X' 00'					書き込み アドレス情報	読み込み アドレス情報	LBA/STT
3	データブロック長							

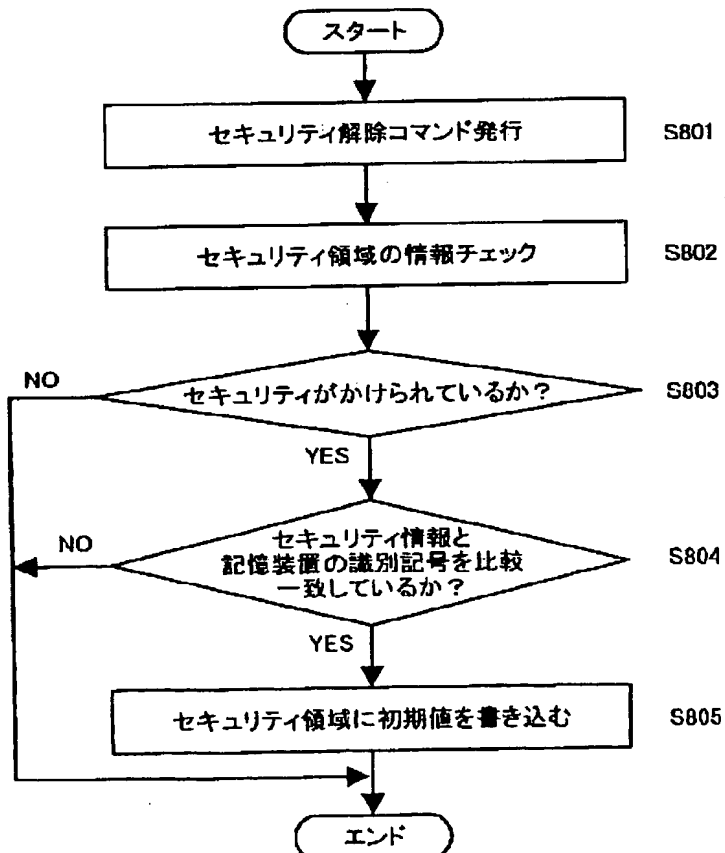
Bit	7	6	5	4	3	2	1	0
Byte								
0	セキュリティレベル							
1	ページコード							
...								
n	パラメタフィールド							

【図8】

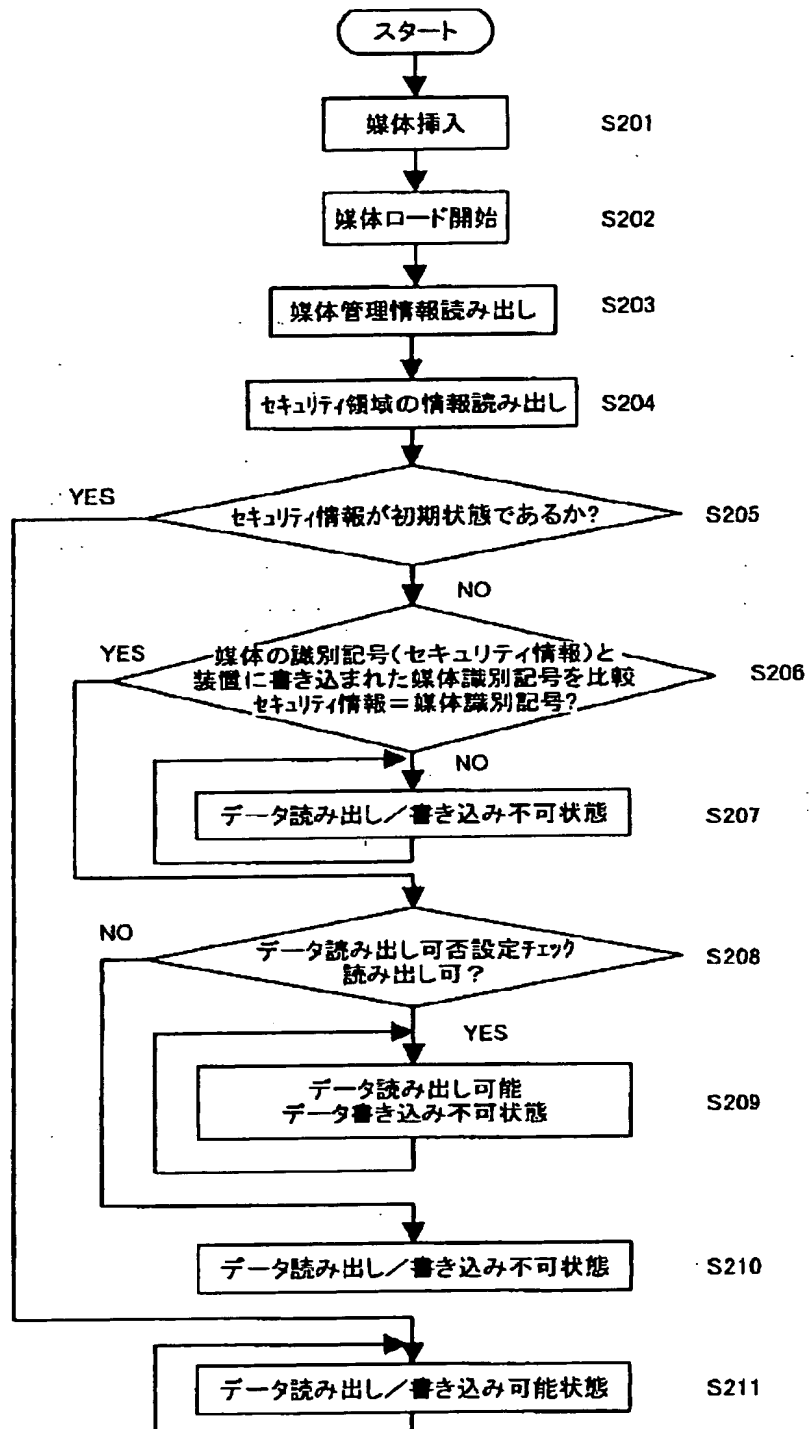
Bit	7	6	5	4	3	2	1	0
Byte								
0	X' 01'							
1	X' 01'							
2~22	パスワード							

Bit	7	6	5	4	3	2	1	0
Byte								
0	X' 01'							
1	X' 02'							
2	ページ番号							
3~6	セキュリティ LBA							
...								
n~n+3	セキュリティ LBA							

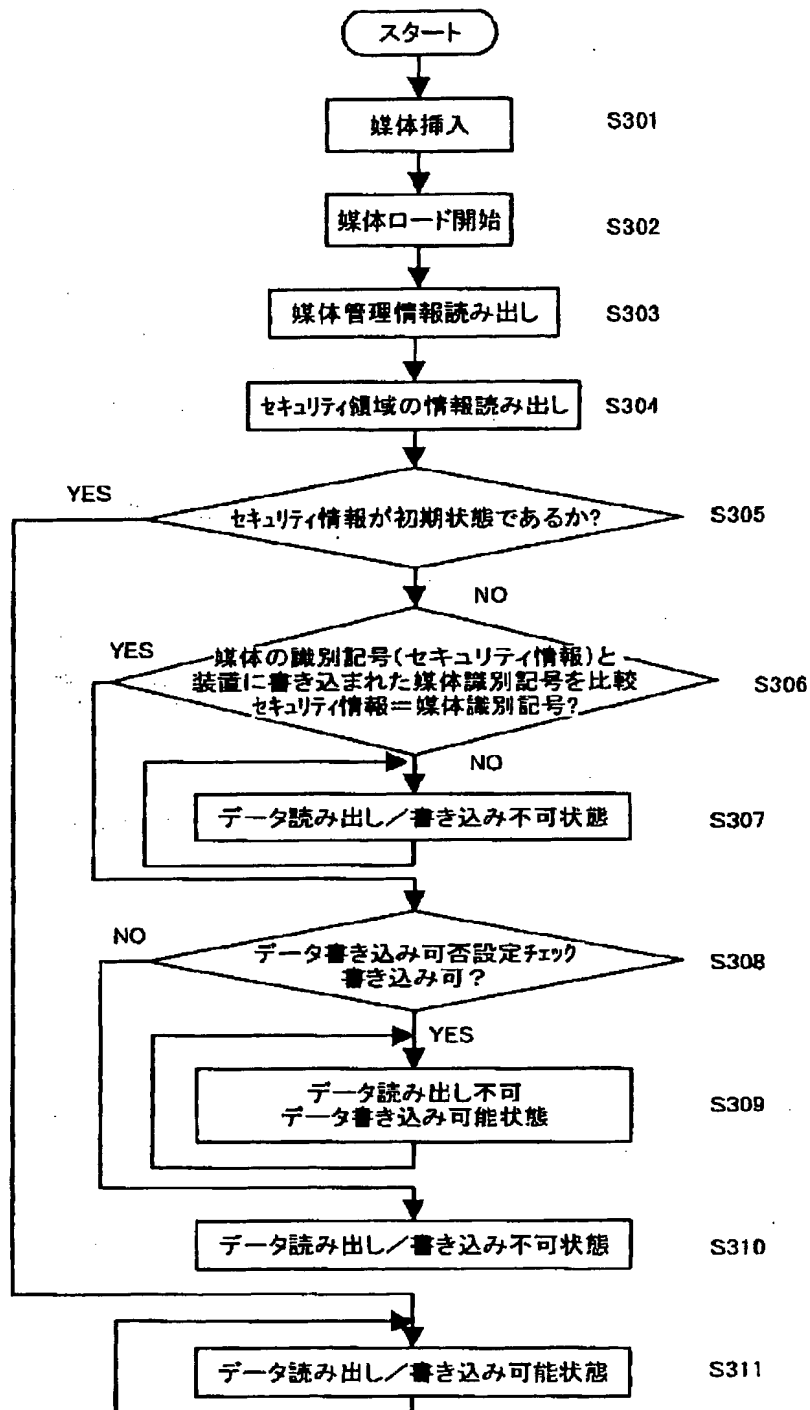
【図15】



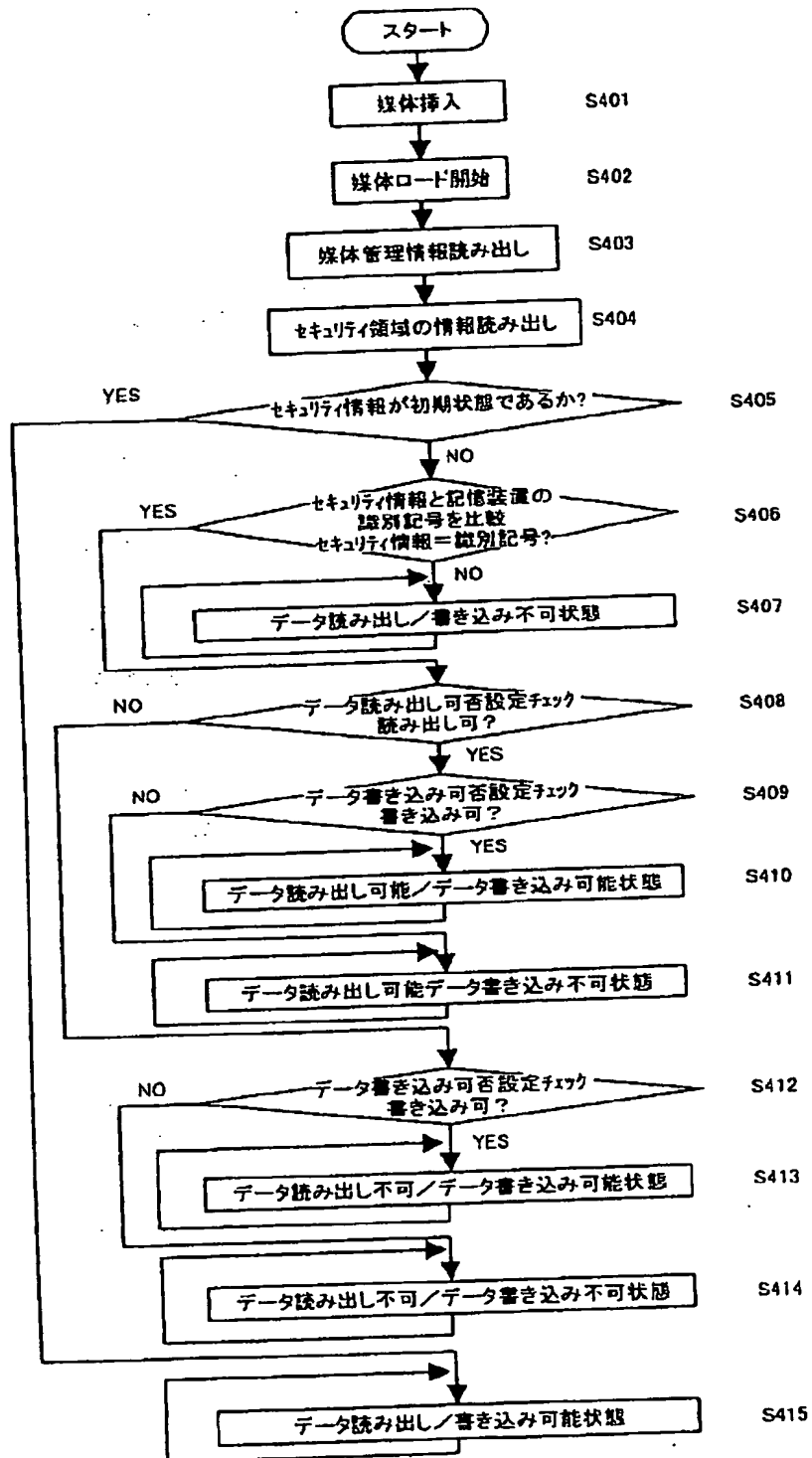
【図9】



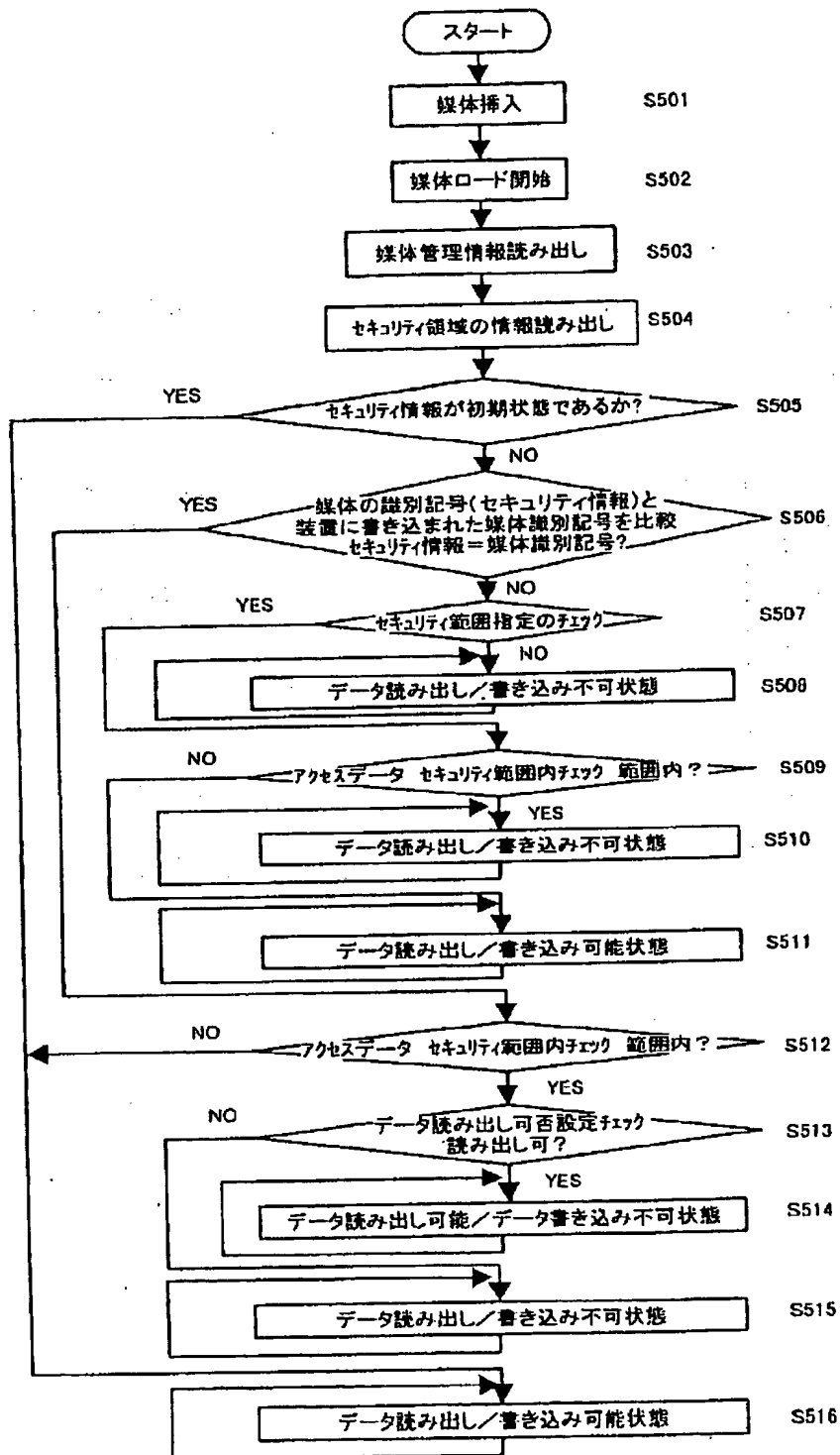
【図10】



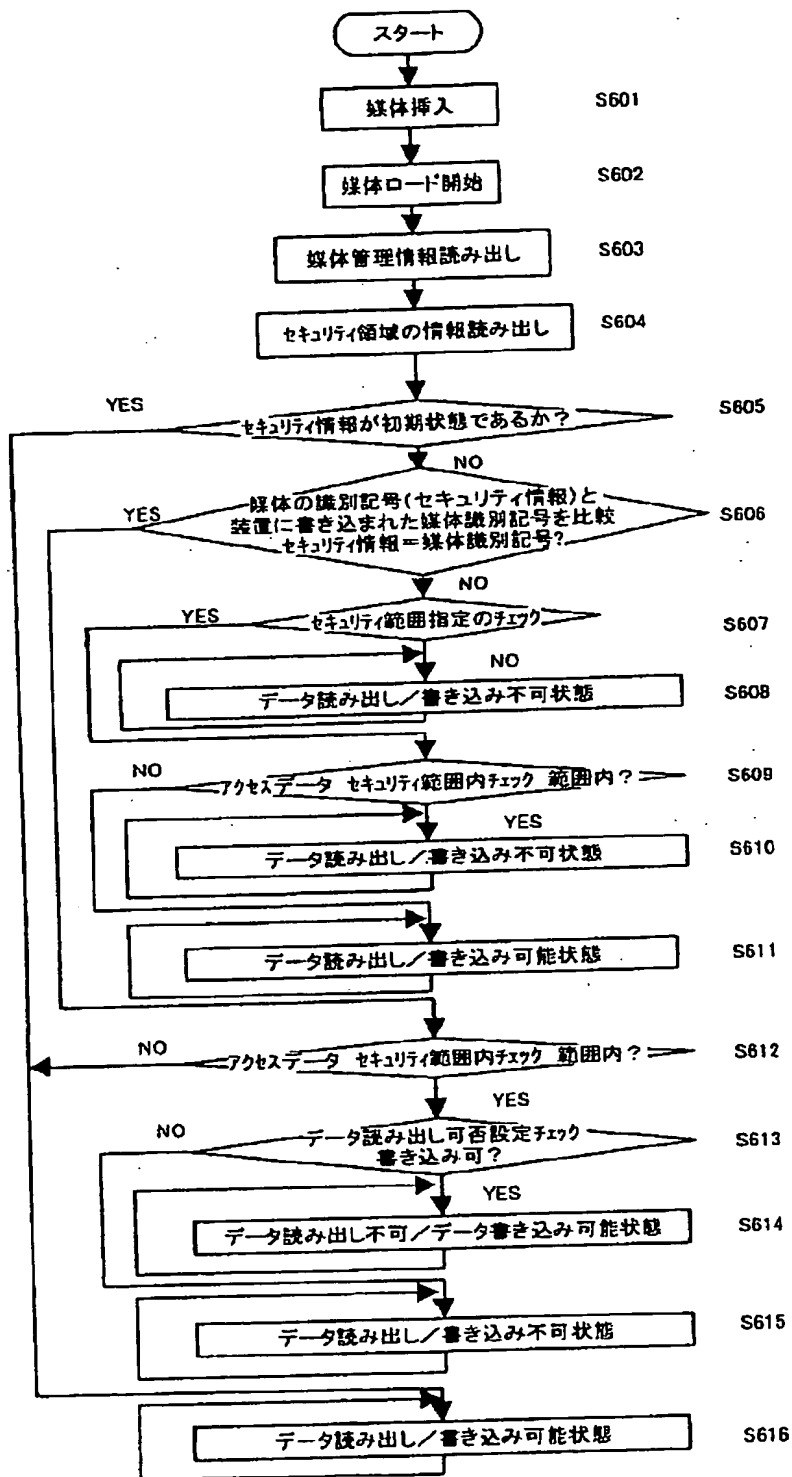
【図11】



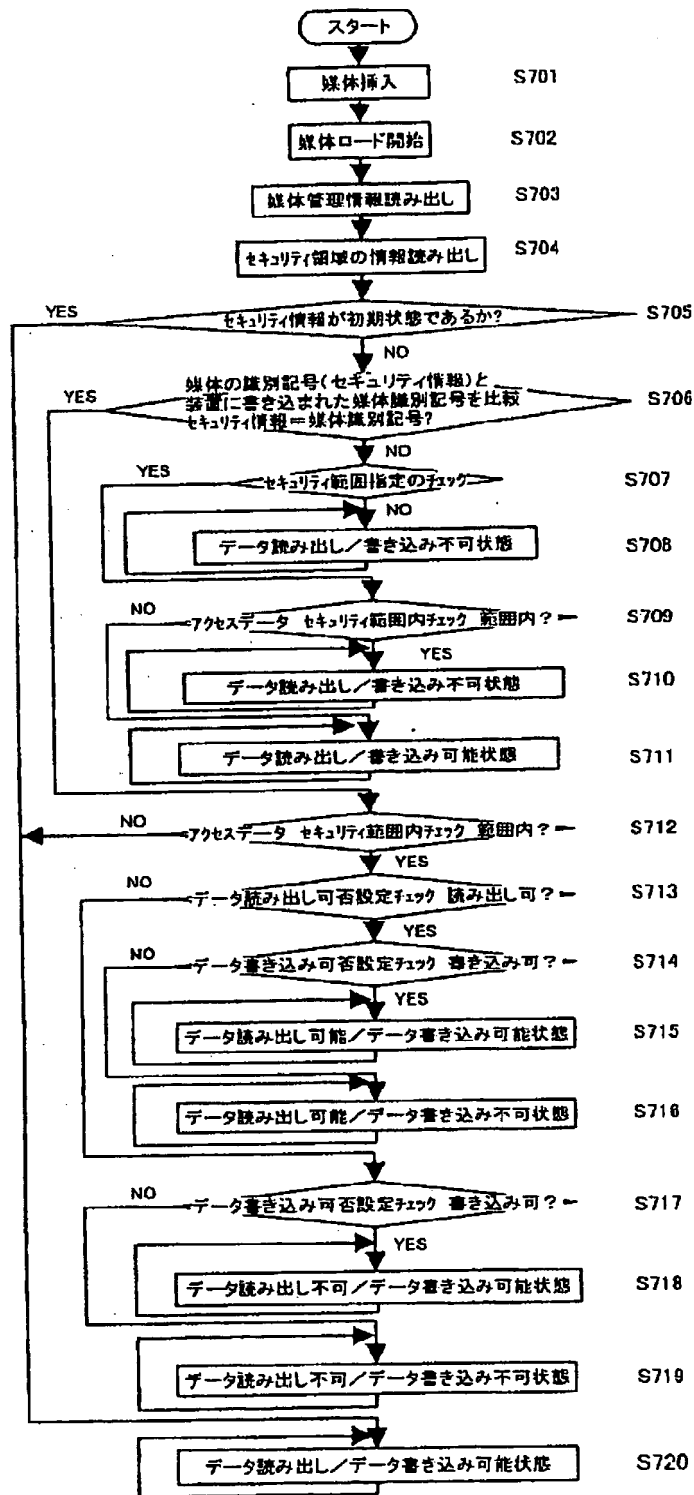
【図12】



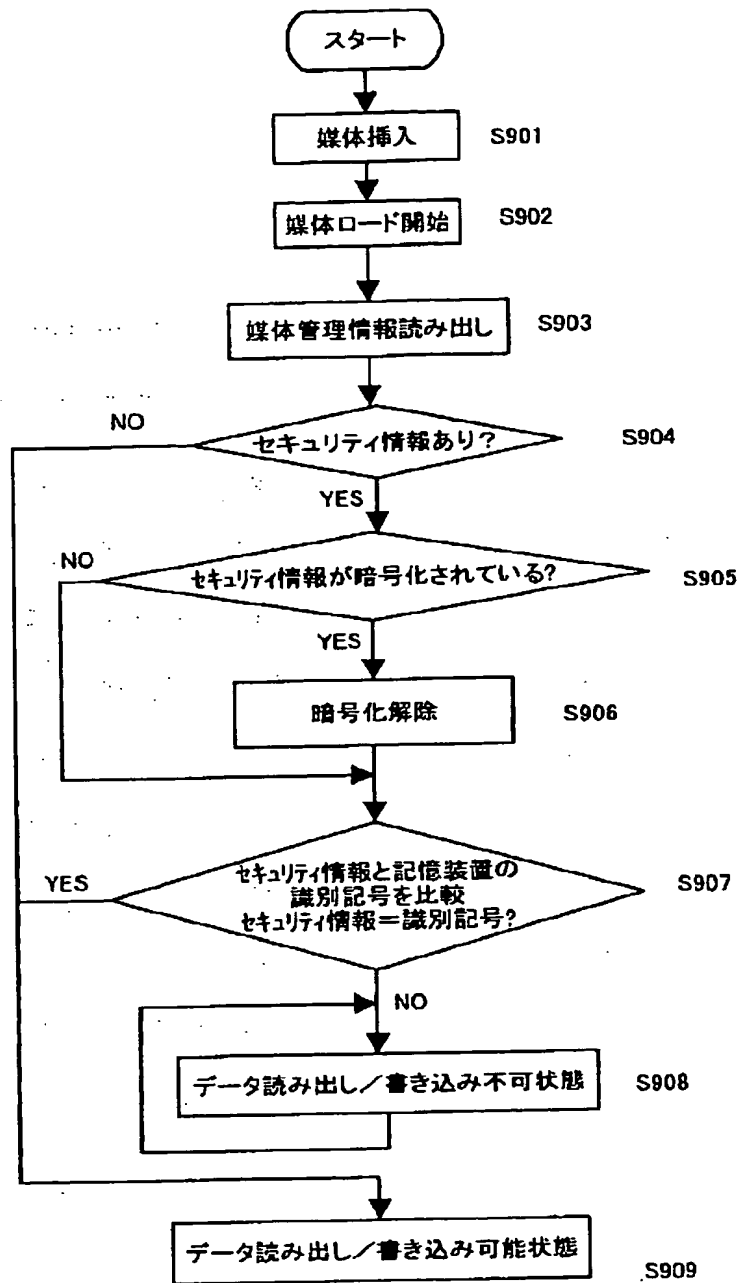
【図13】



【図14】



【図16】



【図17】

